



RESEARCH DEPARTMENT



REPORT

A conditional
access system for
direct broadcasting
by satellite

S.M. Edwardson, C.Eng., F.I.E.E.

A CONDITIONAL ACCESS SYSTEM FOR DIRECT BROADCASTING BY SATELLITE

S.M. Edwardson C.Eng. F.I.E.E.

Summary

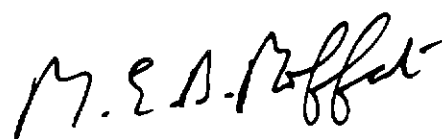
Work is in progress throughout the world in connection with the setting up of systems for Direct Broadcast by Satellite (DBS). The need for the financing of such systems and the services they will carry has led to the conclusion in some countries that they will be of the "Conditional Access" kind. This means that they will carry signals that will be scrambled and be recovered only by users who have paid the necessary charge and whose receivers thereby contain the necessary descrambling key.

The object of this Report is to outline the main features of a proposed Conditional Access television system. The proposal is described in the context of DBS but it is also applicable, in principle, to terrestrial broadcasting or cable operation, although there would be technical differences between the various applications. The possibility that some users of a DBS service might receive their signals via a cable system (the cable-head being fed off-air) raises some problems of compatibility that have not yet been fully resolved and these are discussed in the report.

The proposal outlined is based upon the need to preserve security, to provide a 'user-friendly' operation and to minimise the size of back-up organisation. The Report outlines, first, a basic system and then goes on to describe a number of variants and options that might be possible. The special problems of security, in circumstances where several different broadcasters may be operating, are examined in relation to the user's need for simplicity and reliability. The Report describes a practical solution in which customised induction-coupled sub-systems would be used in domestic receivers to control the provision and use of keys for descrambling.

It is concluded that the proposal could form the basis of an operational service.

Issued under the Authority of



Head of Research Department

**Research Department, Engineering Division,
BRITISH BROADCASTING CORPORATION**

November 1986
(EL-183)

This Report may not be reproduced in any form
without the written permission of the
British Broadcasting Corporation

It uses SI units in accordance with B.S. document
PD 5686.

A CONDITIONAL ACCESS SYSTEM FOR DIRECT BROADCASTING BY SATELLITE

S.M. Edwardson C.Eng. F.I.E.E.

Section	Title	Page
	Summary.....	Title Page
1.	Introduction.....	1
	1.1. General.....	1
	1.2. Receivers	1
	1.3. Scrambling.....	1
	1.4. Encryption	1
	1.5. Descrambling without transmission of encryption data	3
2.	Picture signal scrambling	3
3.	Sound signal scrambling	5
4.	The user's point of view	5
5.	Computer-control	6
6.	Outline of a possible system	6
	6.1. Overall arrangement	6
	6.2. Cost of the back-up organisation	6
	6.3. Security.....	6
	6.4. Number of broadcasters and further security aspects	8
7.	A practical detachable sub-system	9
8.	Other options.....	10
	8.1. Prepaid sub-systems	10
	8.2. Over-air credit	10
	8.3. Telephone direct-debiting	10
9.	Conclusion	10
10.	Acknowledgements	10
11.	References	11

© BBC 2006. All rights reserved. Except as provided below, no part of this document may be reproduced in any material form (including photocopying or storing it in any medium by electronic means) without the prior written permission of BBC Research & Development except in accordance with the provisions of the (UK) Copyright, Designs and Patents Act 1988.

The BBC grants permission to individuals and organisations to make copies of the entire document (including this copyright notice) for their own internal use. No copies of this document may be published, distributed or made available to third parties whether by paper, electronic or other means without the BBC's prior written permission. Where necessary, third parties should be directed to the relevant page on BBC's website at <http://www.bbc.co.uk/rd/pubs/> for a copy of this document.

A CONDITIONAL ACCESS SYSTEM FOR DIRECT BROADCASTING BY SATELLITE

S.M. Edwardson C.Eng. F.I.E.E.

1. Introduction

1.1. General

A great deal of work is in progress throughout the world in connection with the setting up of systems for Direct Broadcasting by Satellite (DBS). The need for the financing of such systems and the services they will carry has led to the conclusion in some countries that they will be of the 'Conditional Access' kind. This means that they will carry signals that will be scrambled and be recovered only by users who have paid the necessary charge. Such a charge might be in the form of a single regular subscription. Alternatively, one subscription could cover most programmes, with an additional subscription to cover, for example, a second 'tier' of special or 'premium' programmes during the period concerned. 'Impulse Pay-per View' is also possible.

This Report outlines the main features of a proposed Conditional Access television system. The proposal is described in the context of DBS¹ but is also applicable, in principle, to terrestrial broadcasting or cable operation, although there would be technical differences between the various applications. The possibility that some users of a DBS service might receive their signals via a cable system (the cable-head being fed off-air) raises problems of compatibility that have not yet been fully resolved and these are discussed in the Report.

The proposal outlined is based upon the need to preserve security, to provide a 'user-friendly' operation and to minimise the size of the back-up organisation. The Report outlines, first, a basic system and then goes on to describe a number of variants and options that might be possible.

1.2 Receivers

In the early years of a DBS service, it is likely that direct domestic reception will be achieved in one of two ways. First, because many existing viewers will not wish to replace their present 'terrestrial' television receivers, special adapters will be used to receive and convert the DBS signals to a form suitable for feeding to the existing receivers. Second, a new kind of integrated receiver will become available, capable of receiving both DBS and terrestrial services.

For the purposes of this Report, the method of reception is of no consequence and the term 'receiver' may be taken to apply either to the adapter unit or to the integrated receiver.

1.3 Scrambling

The term scrambling is used to describe the process to which the transmitted signals are subjected in order to render them unusable in their scrambled form. A complementary descrambling process is used at their receiver to recover the original signals. It is regarded as essential that the finally reproduced signals should show no impairment attributable to the scrambling and descrambling processes.

Although the picture and sound signals will normally be scrambled, it must also be possible to transmit and receive without scrambling, in which case the picture and sound signals will then be available on the receivers of non-subscribers. An interesting alternative to this requirement has been proposed and is under consideration both in the UK and other European countries. This is the idea that all DBS picture signals should be scrambled, whether the service they are part of is in the conditional-access or free-access category. The advantage to be gained from the universal use of picture signal scrambling is found in the reduced visibility of interference and the consequent reduction in protection ratios of up to about 2 dB that results. In deciding upon the methods of scrambling to be used, attention must also be paid to the need to keep receiver costs as low as possible and it is thought that universal scrambling might result in some economy of scale in this important area.

1.4 Encryption

The term encryption is used here to describe the process of enciphering* of the descrambling control signal that is transmitted together with the scrambled picture and sound signals, so as to enable a receiver to describe and reproduce them. At the receiver, the encrypted control signal is decrypted using a secure 'Authorization Key' (a multi-digit

* The word 'encryption' is the American equivalent of the British word 'enciphering'. The American word is chosen because of its common use in the literature.

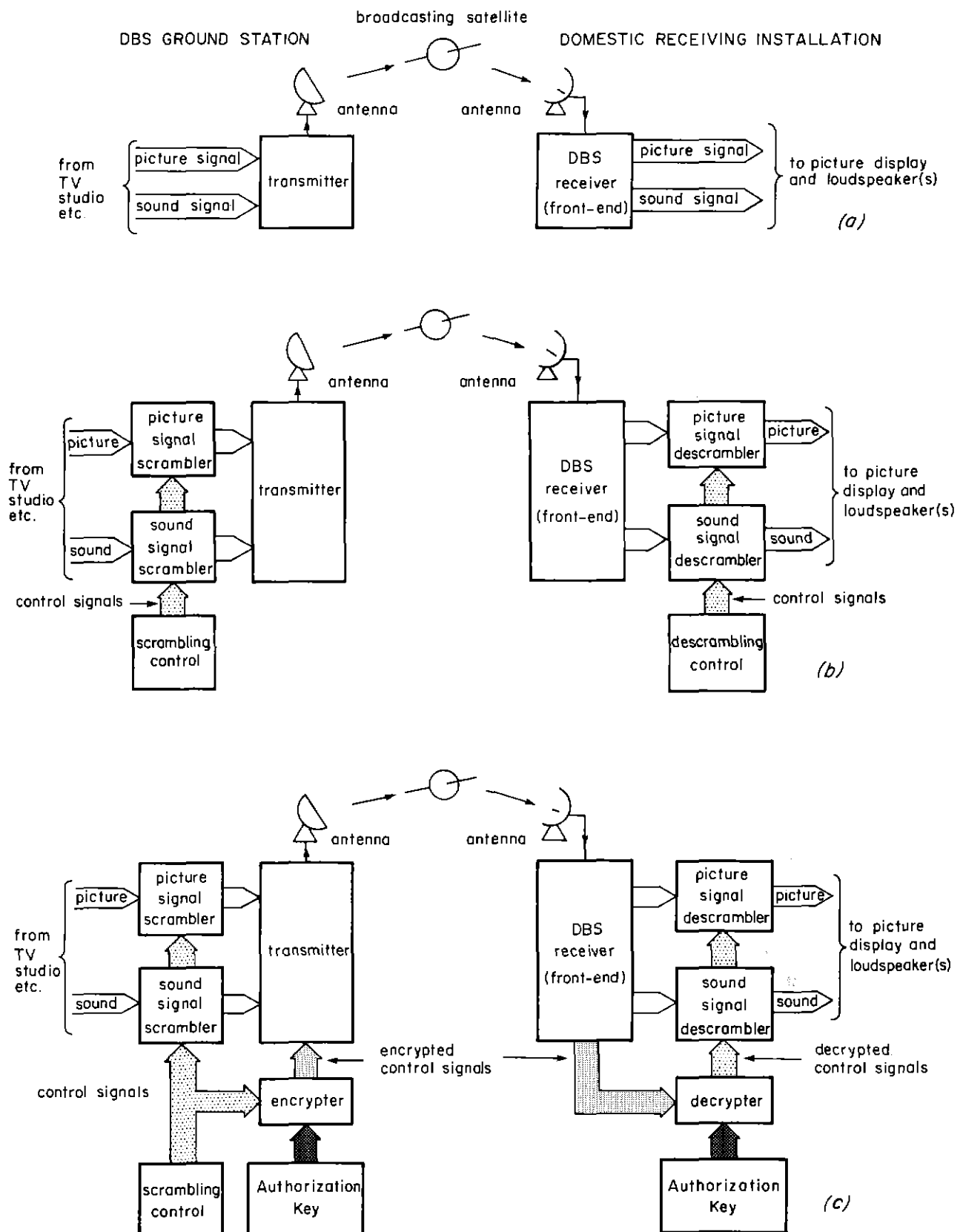


Fig. 1 - DBS: Scrambling and Encryption;
 (a) Basic Arrangement; (b) With Scrambling; (c) With Scrambling and Encryption.

number) and a flow of control signals then passes to the descrambling circuits so as to recover the original picture and sound signals. The provision and protection of the Authorization Key are very important and are described later. In 1982, it was estimated that, by tampering with decoders, between 10% and 25% of PAY-TV viewers in the USA were avoiding paying for their services.²

The way in which scrambling and encryption might be embodied in a DBS system is shown in step-by-step form in Fig. 1(a) to (c). Fig. 1(a) illustrates some of the basic elements. Fig. 1(b) shows the addition of scrambling to the picture and sound signals; in this case, a predetermined and fixed scrambling process would be used. Fig. 1(c) now shows the means whereby the control signals are carried in encrypted form to the receiver, where they are decrypted (using the inverse process and exactly the same Authorization key as at the transmitter) and used for descrambling the picture and sound signals for reproduction. In a practical application, the encrypted signals would be carried in the data channel provided in the digital sound multiplex component of the DBS signal; in non-DBS applications, special provision would be necessary for this data signal.

1.5 Descrambling without transmission of encryption data

Fig. 2(a) shows a simplified version of the arrangement already seen in Fig. 1(c). Now consider the re-arrangement shown in Fig. 2(b). Here the scramblers and descramblers are both driven by identical 'encrypting' devices and the data itself is transmitted 'plain text' (i.e. without encryption) via the data channel. That we are able to do this arises from the special nature of the signals themselves which, unlike other secret information, require only that they should be unpredictable by means other than those at the receiving end. Taking the process a step further, with reference to Figure 2(c), we have identical generators at the sending and receiving end each driving identical 'encrypters', synchronism being obtained by means of the television signal itself; in practice, the 28-bit Frame Count signal used in DBS is very convenient for the purpose.¹

The chief advantages gained from this arrangement are:

- (i) No data channel is required for this purpose.
- (ii) There is no need for a decrypting process at the receiver. This means that the 'encrypting' device can now be a simpler one-way function (a function whose inverse should take a prohibi-

tively long time to compute) and which does not need to be a true encryption device.

Work on DBS in the EBU has resulted in the detailed specification¹ of the signals to be transmitted as part of the encryption system and the EBU nomenclature is used whenever possible in this Report. However, in cases where clarity may not otherwise have been preserved, simpler and more self-descriptive terms are used. For example, the words 'encrypted descrambling control signals' are used in preference to 'Entitlement Checking Messages', as used in the EBU specification.¹ This choice does not constitute an implied criticism of the EBU specification but is rather a consequence of the fact that this Report does not need to contain the detail or range of options that are covered by the EBU specification.

2. Picture signal scrambling

After considering a number of picture signal scrambling methods, one based upon the French Discret 2 system³ was chosen. In this method, known as Component Rotation*, each television picture line signal component is cut at one of 256 points, the position of the cut being selected according to a pseudo-random number sequence. The two segments, so formed, of each component are then interchanged (rotated) left to right.^{1,4}

This method combines a number of advantages,

- (i) Opacity: In scrambled form, the structure of the original picture is virtually destroyed and no useful picture information can be discerned.
- (ii) Security: The method is highly resistant to piracy.
- (iii) Transparency: Impairments attributable to the scrambling/descrambling processes are normally imperceptible.

Against these must be set the following disadvantages,

- (iv) Special circuits: time-redistributing circuits are required in the receiver. However, the introduction of digital video signal processing in domestic PAL television receivers^{5,6} is expected to make a valuable contribution in this respect. Furthermore, the adoption of MAC (Multiplexed Analogue Components)¹ leads to circuitry which will readily lend itself to this kind of signal processing.

* Originally known as 'Active Line Rotation' when applied to PAL, SECAM, or NTSC signals.

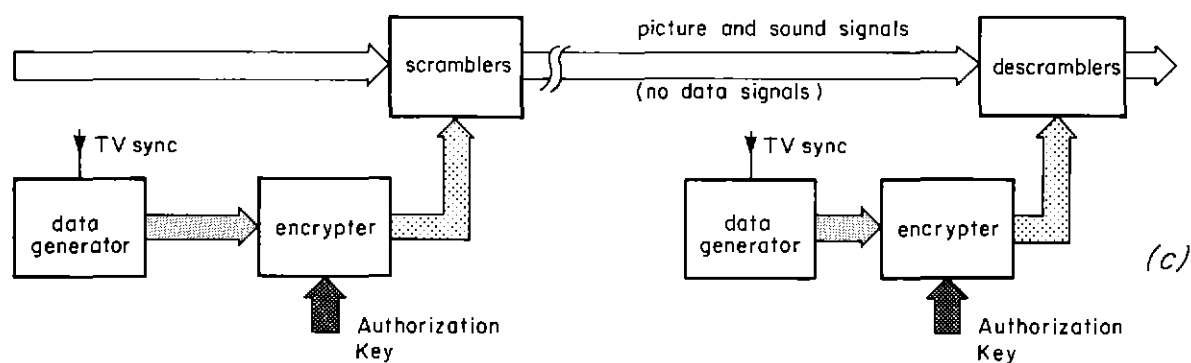
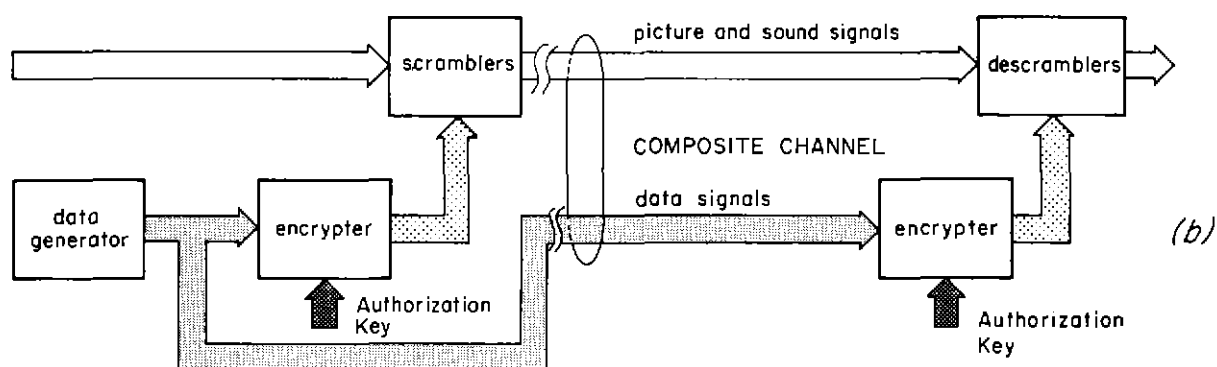
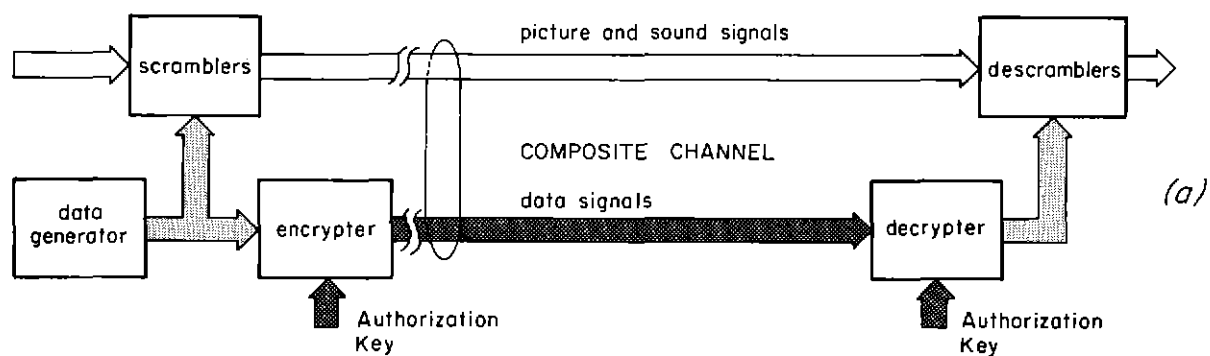


Fig. 2 – Operation without transmission of encryption data;
 (a) With Encryption Data (b) With Plain text Data; (c) Without Data.

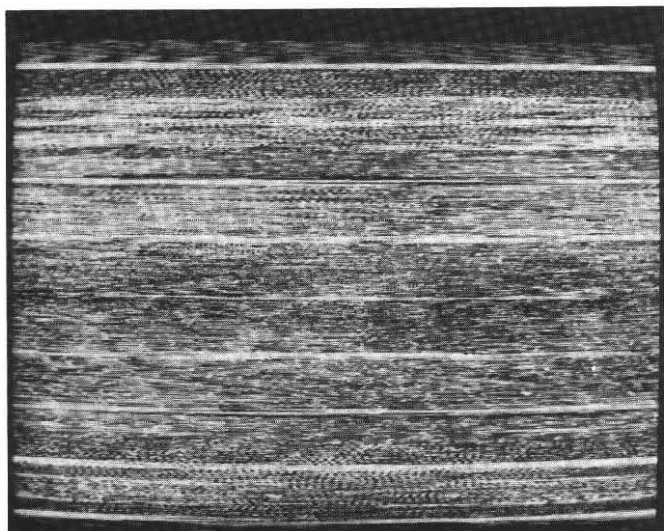


Fig. 3

(v) Line tilt: the tolerances on transmission and receiver distortions are somewhat tighter than for non-scrambled picture signals. This aspect has received study and results so far have not revealed any difficult or expensive problem as far as DBS (f.m.) signals is concerned. However, there is a possibility that some users might receive their signals via existing cable systems and simulation tests carried out by the IBA in the United Kingdom have indicated that the tolerances on their performances might be insufficiently tight. In particular, the common use, on cable, of v.s.b./a.m. can give rise to amplitude/frequency distortion at low video frequencies that can cause 'line tilt' effects which can appear as low-frequency noise on the descrambled picture. The addition of unwanted line-frequency 'sawtooth' components, possibly due to clamping imperfections, is another cause of line tilt.

In the component-rotation method, with MAC signals,⁴ the colour-difference and luminance components are separately rotated and separate independent cut points may be used for each. The photographs in Fig. 3 show a scrambled picture and the picture obtained after descrambling. As already stated, the locations of each of the two cut points on any line in the picture can have any one of 256 positions and each location can thus be described by an 8-bit binary number. In practice, a pseudo-random binary sequence (p.r.b.s.) is generated and delivers two 8-bit words per television line to the scrambler circuit. At the receiver, an identical p.r.b.s. generator runs in synchronism with that at the source and drives the descrambler in the same way. Synchronism is achieved by the use of a time marker¹ in conjunction with the encryption data

which provides regular initialisation data words for the p.r.b.s. generator.

3. Sound signal scrambling

The digital sound multiplex system adopted by the EBU¹ employs a form of packet system for the transmission of the digital television sound and other sound signals, as well as data signals. Whilst the scrambling of a digital signal is inherently easier than the scrambling of an analogue signal, the use of a packet-multiplex system has necessitated the solution of special problems, particularly in achieving synchronism between the sound scrambler at the source and the receiver descrambling circuits.

The basic scrambling method is to add, by modulo-2 addition, a p.r.b.s. signal to the original digital sound signal. At the receiver, exactly the same process results in recovery of the original signal.

4. The user's point of view

It is useful first to look at one form of the basic method from the point of view of the user; other alternatives are described later. We assume that all the DBS equipment has been installed and operates satisfactorily. The following sequence could occur.

- (i) The user would make his first payment.
- (ii) He would then receive a detachable sub-system, perhaps like a rectangular plastic block or card, that would fit into his receiver, out of sight, perhaps in a small drawer. The sub-system would contain processing circuitry, together with an electrically embedded Address and a Distribution key, unique to the subscriber, in the form of multi-digit numbers.

- (iii) A Validation Signal, also a multi-digit number, would be delivered 'over-air', addressed to the sub-system in the viewer's receiver and the receiver would then reproduce the (descrambled) picture and sound signals; the viewer would not otherwise need to be aware of the fact that the Validation Signal had been delivered.
- (iv) Further payments, say at monthly intervals, would result in the over-air delivery of new Validation Signals which would maintain the service. The original sub-system would continue to be used in the receiver.
- (v) Failure to make a due payment would result in no issue of a new Validation Signal, with consequential cessation of the service (and the appearance of scrambled picture and sound*) on expiry of the current period; subsequent payment would result in the issue of a Validation Signal, delivered 'over-air' to restore the service.

5. Computer-control

It is evident from the foregoing that a back-up or service organisation will be needed to receive payments from the public and to issue and deliver the customised sub-systems and Validation Signals to subscribers. In the method proposed here, it is envisaged that this would be computer-based with a minimum of human intervention.

The computer would have two linked parts. One part would constitute a data-base in which all subscriber-related data would be stored and processed. Its output of Validation Signals would be distributed by over-air-addressed transmission to subscribers. The other part would provide scrambling-control and key-signals (multi-digit numbers) for use by the DBS Ground Station or other signal origination point. Because of the need for security, these signals would have to be protected and for this reason it would be preferable for the Control Computer and signal origination point to be co-sited.

The use of computer control would bring two main benefits:

- (i) Security: the process of generating both the Authorization Keys and the Validation Signals would be buried within the mechanism of the computer and no human access would be needed, except as an executive input to 'enable' the distribution of sub-systems and Validation Signals to users.

* Receiver designers could arrange for 'blank screens and silence' under these conditions.

- (ii) Economy and Reliability: Useless great care were taken, the back-up or service organisation could become very large indeed. The use of computer control would allow almost complete automation of all operations downstream from the human operator. (Upstream from this point, it would be necessary to provide payment-receiving facilities, as well as the other associated interfaces with the public. This could perhaps include multiple remote terminals if this were found desirable and did not introduce a financial security problem).

6. Outline of a possible system

6.1 Overall arrangement

Fig. 4 shows one overall arrangement and is derived from Fig. 1(c), with the addition of the computer and the sub-system.

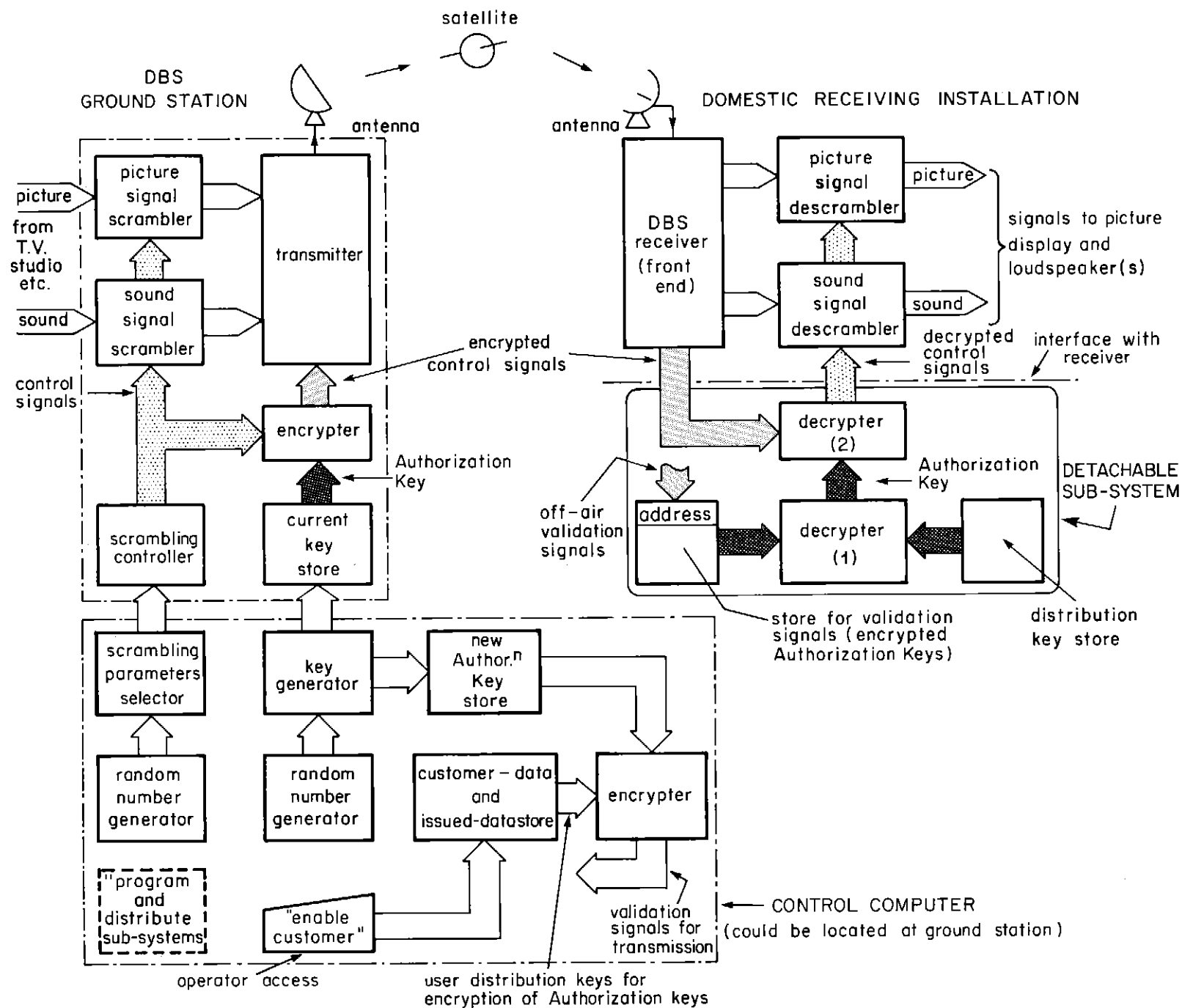
The detachable sub-system would contain micro-circuits. However, since it would not need to be carried in a wallet, it could be bulkier than a bank card although it would still need to be convenient and cheap to post. All sub-systems would be physically identical, but each would carry a unique embedded Address and Distribution Key (or Keys), written-in by the computer when they were first programmed before distribution to the customers; these would also be stored in the data-base against the customer's name, etc.

To obtain a Validation Signal destined for transmission to a particular customer, the appropriate Authorization Key would be encrypted at source, using the customer's (sub-system) unique Distribution Key as the encryption key. At the receiver, when the Validation Signal had been received, the Authorization Key would appear at the output of decrypter (1) in the sub-system, the 'off-air' Validation Signal having been decrypted using the Distribution Key. The form of the encryption/decryption process or algorithm is outside the scope of this Report.

Summarising,

- At any given time, the broadcast control signals would be encrypted at the transmitter using a secure Authorization key; the same value of Authorization key would be derived in all receivers to enable the encrypted control signals to be decrypted and descrambling to be achieved.
- The Validation Signal delivered to each receiver's sub-system would form a unique combination with the Distribution Key already embedded in the sub-system, thereby to decrypt

Fig. 4 - Example of Overall Arrangement.



the Validation Signal and obtain the Authorization Key.

- The control computer would automatically determine both the scrambling parameters and the values of the keys required. The generation of these values would be based upon random numbers.

6.2 Cost of the back-up organisation

Most of the costs would be incurred in dealing with the public; this would be mainly in the handling of incoming mail and telephone calls, since the output of sub-systems and signals would be almost fully automated. It is estimated that, assuming monthly payments, the annual cost per customer would be £4.50.

6.3. Security

When considering security, the potential pirate is regarded as operating on a substantial scale; this would seem to be necessary to justify the considerable outlay likely to be required.

The scrambling and encryption processes may for convenience be regarded as separate. Thus, two basic approaches are open to a potential pirate

- (i) He can attempt to reconstruct the original picture and sound signals, using only the scrambled signals themselves and independently of the encryption data.
- (ii) He can attempt to find the Authorization Key and thereby decrypt and derive the control signals for the descrambling circuits to recover the original signals.

As regards the first approach, such piracy would probably involve the construction of special and rather expensive additional hardware that would require clandestine marketing and installation.

Although the first method should not be disregarded, it is felt that a more determined effort at piracy might be made through the second approach, which would involve software only and could be cheaper and less obtrusive. It is not possible, here, to detail the kinds of attempt that might be made to find the key. However, a trial-and-error method seems unlikely to be attempted.

The copying or 'cloning' of a legitimately obtained sub-system is a serious possibility. If a large number of cloned systems were made and sold by a pirate, one single payment for a service would be sufficient for that same service to be received by all

the pirate's 'customers'. This form of attack would be difficult to detect but counter-measures are described below that would cause the service to be terminated and the pirate to lose credibility with his customers, without the identity of either the pirate or his customers needing to be known.

An alternative method that might be attempted would involve a breaching of the security of the broadcaster's data-base.

6.4 Number of broadcasters and further security aspects

It is likely in the future that more than one broadcasting authority will provide pay television services for reception in the same country and the question then arises as to how best to organise and co-ordinate the various operations to provide both a secure and user friendly system. The requirements and possibilities may be listed.

- (i) The basic methods of picture and sound signal scrambling (and descrambling) require to be standardised and the same methods used by all broadcasters. Failure to achieve this would result in either or both very expensive receivers and only partial cover of a given population by some programmes. Standardisation of this aspect has already been achieved for DBS in Europe.¹
- (ii) Each broadcasting authority could program and issue its own sub-systems, as already outlined. These would be unique to each subscriber, with the embedded Addresses and Distribution Keys also being stored only at the data-base of the particular issuing authority. This method has the security of a single data-base for each broadcasting authority, with the advantage of retaining independent control over its own conditional access system; a broadcaster could, for example, introduce independent anti-piracy measures without reference to any other. The use of detachable sub-systems brings two important advantages. First, the flexibility to introduce new facilities and services. For example, new pre-payment methods and additional conditional access services could be introduced simply by providing the appropriate sub-system. Second, the issue of new sub-systems could be used to wipe out automatically any existing piracy of the kind based on the cloning of sub-systems, whether the identity of the pirate was known or not. On the other hand, the domestic user may be faced with the confusion of handling several different sub-systems, a situation that could lead to dissatisfaction and unreliability. To help in this dif-

ficulty, the receiver must be designed to work easily and smoothly with several conditional access systems and a practical approach on these lines is described later.

- (iii) A single sub-system could be used that would be designed to handle the conditional access services of all broadcasters. This would mean that, although the sub-system might have more than one mode of operation, all authorities would use the same basic circuit and have access to the embedded codes, (although they would not, of course, use the same Authorization Key) and there would need to be a common or shared data-base. This approach is simpler and better for the user than (ii), but is likely to be less secure because of the larger number of organisations with access to the data-base.
- (iv) Taking the simplification of (iii) even further, the use of a separate detachable sub-system could be dispensed with altogether and the necessary customised circuits could be embodied or 'buried' permanently in the receiver.⁷ The simplification and economy thus gained are obvious and attractive, but two disadvantages can be foreseen, in addition to the security problems of data sharing outlined in (iii) above.
 - (a) Programming or 'customising' of the receiver itself would now be needed, perhaps at the factory, and this could lead to further loss of security, as well as commercial and marketing problems.
 - (b) Without a detachable sub-system, the receiver's embedded codes and decryption circuits would be built-in and could not be changed, thus removing both flexibility and an important

anti-piracy weapon from the hands of the broadcaster. In this context, it is important to realise that time may be on the side of the pirate. The sophistication of technology is continually improving and its real cost is decreasing. Whilst the broadcaster is under pressure to finalise certain parameters now, in 1986, the pirate is unlikely to begin operations until a large DBS audience is available, say by the 1990s. It is thus advisable for the broadcaster to fix, unalterably, as little as possible so as to retain a maximum of flexibility and manoeuvrability.

7. A practical detachable sub-system

In the previous section the advantages were outlined of using detachable sub-systems. Whilst there is a very strong case for this, and at least one version is available commercially in the form of the ingenious French Smart Card⁸, the practical disadvantages at one time seemed to be overwhelming. For example, problems with contact reliability were thought likely to be serious. The sub-system will probably remain fixed in position for a very long time, perhaps for several years, and in this case the contacts would not receive the necessary cleaning 'wipes' that are normally required. Moreover, any receptacle or slot in the receiver could become contaminated with foreign bodies which would worsen these problems. A further requirement might be the need for a receiver to hold several sub-systems at a time for several services, perhaps as many as six, and the notion of a receiver simultaneously carrying six plug-in sub-system units using electrical contacts is not an attractive one. Above all there exist the important needs of low cost and user convenience.

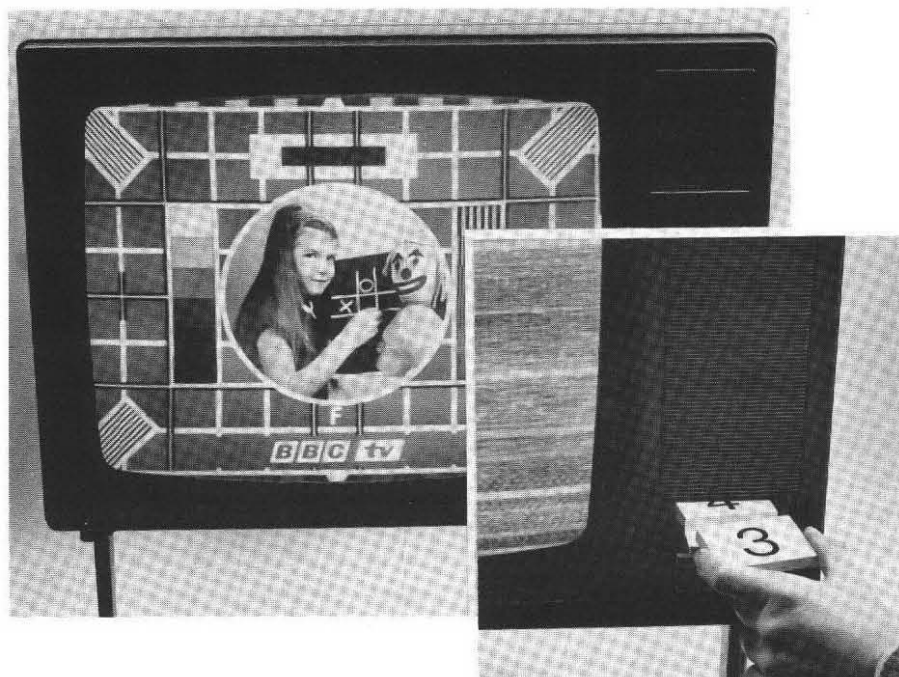


Fig. 5 – Experimental Induction-coupled Detachable Sub-system.

Of the various alternatives that were considered, an induction-coupled sub-system has been developed in experimental form, in co-operation with a commercial manufacturer. Induction-coupled devices have several advantages:

- (i) There are no external electrical contacts either in the receiver or on the detachable devices and their elimination makes induction-coupling particularly suitable for the hostile environment presented by domestic television receivers.
- (ii) Inserting or removing the sub-systems is very simple for the user. The experimental unit described here and seen in Fig. 5 uses a small drawer in the receiver similar to the drawer carrying the tuning controls. The sub-system units, which are small rectangular blocks, can be placed in the drawer without special regard to their exact position.
- (iii) The system can accommodate several sub-systems simultaneously for use with independent conditional access services.

The experimental unit was built to demonstrate the basic principle and employed the same techniques that would be used in an operational unit. In the model, a micro-processor is used to convert data from the receiver into a form suitable for transmission to the detachable sub-system. The data is modulated onto a carrier which drives a coil located around the drawer unit and the appropriate device in the drawer responds to the transmitted data by returning processed data modulated onto a second 'return' carrier. A microprocessor takes this data from the receiving coils, performs error protection and delivers a descrambling control word to the p.r.b.s. generator in the receiver. Each experimental unit is a small rectangular block about 10 × 50 × 65 mm ruggedly encapsulated in epoxy resin. It contains a transmitting and receiving coil and circuitry, power for which is taken from the transmitted carrier itself. There is no internal power source and no external connection.

The drawer was able to contain up to four sub-systems. With large scale future production, the sub-systems would have about one-third of the volume and room for about six would be provided in the receiver. Each would contain a microprocessor and could be programmed to control access to three different services. It is envisaged that each sub-system would be supplied by a particular broadcaster so that the option of controlling three services would not necessarily always be used.

The cost of each sub-system, at 1985 prices and with high volume production, is expected to be similar to the French Smart Card, about £2.

8. Other options

8.1 Prepaid sub-systems

- (i) These could be distributed and sold to the public at such places as Post Offices and banks.
- (ii) They would be inserted into the same part of the receiver and would also operate as a sub-system of it. Such devices could be made and sold as an alternative for those people who might prefer over-the-counter purchases to monthly postal transactions, bank standing-orders, etc.
- (iii) They could contain stored programme-viewing credit (sufficient for a few weeks, say) and would expire on using up this stored credit but would also, necessarily, have an expiry data for security reasons.

It would also be possible to incorporate in the sub-system a programme-logging store in which data concerning the programmes received could be accumulated. After it had been returned to obtain a new one, the programme-logging store could be read and the programme details obtained for 'listener research'. The source of the information would be anonymous since the identity of the user would not be known.

8.2 Over-air credit

The use of over-air addressing is extendible to the transmission of 'viewing credit' to users' receivers and the EBU Specification¹ makes provision for this. It is thought that this method is the one most likely to be used if 'pay-per-programme' facilities are required.

8.3 Telephone direct-debiting

This may be an important option to be kept open for the future when greater penetration by the telephone has been achieved. Here, there would need to be a specially provided link from the receiver via the telephone system to an accounting and control computer and, preferably, also to the user's own bank. Suitable safeguards would be required to protect the user against unwanted debiting and the bank against unwanted withdrawals. The necessary data would be transmitted to the user's receiver in encrypted form via the telephone line. Undue peak loading of the telephone network would need to be avoided when designing the system.

An important property of the telephone connection would be its two-way nature and the flexible, interactive facilities that it would permit.

9. Conclusions

A proposed method has been outlined and it is concluded that it could form the basis for the operation of a conditional access television service in which the broadcast signals would be scrambled and could be received only by those viewers who had paid the necessary charge.

The special problems of security, in circumstances where several different broadcasters may be operating, have been examined in relation to the user's need for simplicity and reliability. It is concluded that a practical solution to these problems would be the use of customised induction-coupled sub-systems in domestic receivers to control the provision and use of keys for descrambling.

The proposal has been described in the context of *Direct Broadcasting by Satellite (DBS)* but is also applicable in principle to terrestrial broadcasting or cable operation, although there would probably be technical differences between the various applications.

10. Acknowledgements

The proposal described in this Report is the result of discussions between a number of the author's colleagues, whose contribution is acknowledged.

11. References

1. EBU, 1984. Television standards for the broadcasting satellite service EBU Doc. SPB 284, 3rd revised version, December 1984.
2. PERR, C.D., 1982. Security and Addressability for PAY-TV. *The Video Revolution*, 1982.
3. CCIR, 1981. Scrambling of Television Pictures by the Discret System. Doc. 11/265 (France), 4 June 1981.
4. KNEE, M.J., 1985. DBS pay television picture signal scrambling BBC Research Department Report No. BBC RD 1985/12.
5. IEEE, 1983. Digital TV makers bet on VLSI. *IEEE Spectrum*, February 1983.
6. ITT, 1983. DIGIVISION, Intermetall Semiconductors ITT technical publication, Edition 1983/3 (no. 6251-209-2E), March 1983.
7. MASON, A.G., 1984. A pay-per-view conditional access system for DBS by means of secure over-air credit transmissions. *International Conference on Secure Communication Systems*, London, 22-23 February 1984. IEE Conference Publication No. 231, pp. 66-70.
8. DAVIES, D.W., 1984. Smart Cards, digital signatures and negotiable documents. *International Conference on Secure Communication Systems*, London, 22-23 February 1984. IEE Conference Publication No. 231, pp. 1-4.

